

AU/AWC/138/1998-04

AIR WAR COLLEGE

AIR UNIVERSITY

**INCREASED MILITARY RELIANCE ON
COMMERCIAL COMMUNICATIONS SATELLITES:
IMPLICATIONS FOR THE WAR PLANNER**

by

Duane A. Jones, Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Victor P. Budura Jr.

Maxwell Air Force Base, Alabama

April 1998

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20011213 084

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

	<i>Page</i>
DISCLAIMER	ii
PREFACE	v
ABSTRACT	vi
FLAGS, BANNERS, BELLS, AND DRUMS	1
MICROCHIPS, SATELLITES, AND CELL PHONES.....	3
A MILITARY COMMUNICATIONS SATELLITE HISTORY	6
In the Beginning.....	6
DSCS	7
FLTSATCOM.....	9
LEASAT	10
Ultra-High Frequency Follow-On.....	11
MILSTAR.....	11
TARGETING OPTIONS	14
Satellite Link (target the flags, banners, bells, and drums).....	14
Ground Link (target the tactical unit commanders)	15
Control Link (target the communications officer)	16
User Link (deafen and blind all the soldiers).....	16
DEFENDING THE RESOURCE	17
Parallel Development Paths	17
Full Circle	18
Security Concerns	20
THE IRIDIUM CASE.....	22
Foreign Control.....	24
Communications Isolation	25
Targeting Ambiguity	25
Geo-location.....	26
Private Proliferation	27
System Dependence	27
Not Just Iridium	28

RECOMMENDATIONS	29
CONCLUSION	30
BIBLIOGRAPHY	32

Preface

The information presented in this research report will be of value to the commander or planner who wants to understand the fundamental security issues associated with the military's migration to commercial communications satellites. As with all emerging technologies, there is a tendency for systems information to become dated before it ever reaches the general audience. For that reason, I've attempted to present concepts rather than specific systems data and believe that the reader can easily apply those concepts to both present and future communications scenarios.

Throughout the writing process, my research advisor, Colonel Victor P. Budura, offered both assistance and guidance. His insights and suggestions are reflected in the pages that follow.

Abstract

The October 1993 Department of Defense Report on the Bottom-Up Review called for a greater reliance on commercial satellites for general-purpose military communications. This policy guidance was influenced in part by the Congressionally mandated Commercial Satellite Communications Initiative (CSCI) studies. As the DOD shifts to commercial platforms, what are the corresponding implications for the war planner? Drawing on information available in the public domain, this paper will attempt to determine whether commercial satellites offer new or increased vulnerabilities; and, if so, suggest new perspectives from which future war planners should view both the protection and denial of satellite communications.

Chapter 1

Flags, Banners, Bells, And Drums

The year is 500 BC, the location somewhere in China, and the warfare theorist Sun Tzu reports that the requirement for effective battlefield communications has been met by the employment of a new technology: flags, banners, drums, and bells.

...when masses of troops are employed, certainly they are widely separated, and ears are not able to hear acutely nor eyes to see clearly. Therefore officers and men are ordered to advance or retreat by observing ¹ the flags and banners and to move or stop by signals of bells and drums.

Can we imagine that this army's opponents may have viewed this communications improvement as a threat? What reactions might this improvement have elicited? Certainly there would have been options. For instance, in an attempt to deny communications the opponent might have decided to target and destroy the flags, banners, bells, and drums making communications to the troops impossible. Perhaps an easier approach might have been to target the communications officer who passed the leader's instructions to the flag and banner bearers, drum, and bell players. Or maybe it would have proved fruitful to attack the tactical unit commanders who received, interpreted, and passed the visual and aural signals to their individual ground troops. Finally, the opponent might have tried to blind and deafen every opposition soldier, rendering the communications useless. Any one of these attack plans would have the effect of denying communications. All are straightforward and easily planned though not

all equally efficient and achievable. The story might end here were it not for a subsequent economic downturn which affected the entire Asian world starting at the end of the last great war. With this downturn came budget reductions that made it virtually impossible for any army to afford its own flags, banners, drums, and bells. Multi-national entrepreneurs appeared who offered cost-effective flag, banner, drum, and bell systems to any and every financially equipped customer. Communications flourished. But over time, enemies began to realize that they all were relying on the same flag, banner, drums, and bell resources. How could an opponent successfully target a system that he relied upon himself? What treacheries were possible if the flag and banner bearers or drum and bell players decided or were compelled to favor one opponent over the other? With this shared communications development, warfare changed forever. It became very complicated; and, those trained in denying the enemy communications prior to the introduction of the merchants found themselves unequipped to effectively prosecute wars. Old approaches to the new challenges proved ineffective and even dangerous.

Simplistic altered fairy tale or allegory for our time? In the following pages we will explore an analogous situation that today challenges our traditional ideas for planning wars: the migration of military reliance from organic to commercial communications satellites.

Notes

¹ Sun Tzu, *The Art of War*, Samuel B. Griffith, Oxford University Press, Oxford, 1963, page 90.

Chapter 2

Microchips, Satellites, and Cell Phones

Second only to the pursuit of improved, more capable weapons, military organizations have traditionally focused on the importance of communication and have invested mightily in its improvement. Today, nearly 2500 years after flags, banners, bells, and drums directed the armies and countless communications systems later, futurists envision that in 2025 communications will be very different. It is thought that the individual soldier will have implanted communications microchips that will be controlled by voice, gesture, or thought.¹

With the progressive improvement in communications technology has come an increased military reliance on communications systems. This reliance has led to a corresponding understanding that denying an enemy's communications is a legitimate and useful, if not essential, military objective. Today's military leaders appreciate this concept and demonstrate that appreciation in their planning and execution of military campaigns. As a recent example, Gulf War air campaign attack planners designated Iraq's Baghdad telecommunications center (known to the CNN-watching world as the AT&T building) as the highest-priority "H-hour" target.² The destruction of that facility was later broadcast worldwide and served not only as an example of precision attack; but

also, as testimony to the importance of denying an adversary vital communications capability.

There is nothing on the horizon that suggests any future change to the fundamental question of whether denying communications to the enemy is militarily important. Planners should and will continue to give priority to this challenge. There is, however, an extraordinary change coming that will force military planners to reassess the "how" of denying communications to the enemy.

Today more than seventy-five percent of overseas military communications are dependent upon satellite links; a remarkable figure when one considers that the advent of the military communications satellite was just thirty-one years ago.³ As communications requirements increase and military budgets decrease, there has been a corresponding, fiscally-motivated congressional interest in increasing military reliance on commercial communications satellites. That interest has translated into new military plans to leverage the commercial communications satellite market. The benefits are many and well documented. The revolution in military thinking that must accompany this transition to civilian satellites is not so well documented. It is essential to understand how this change affects our national vulnerability to communication deprivation as well as our ability to successfully deny our enemies their communications. This paper will introduce leaders and planners to these new concepts and the new ways of military thinking that the migration to civilian communications satellites demands.

Notes

¹ *Alternate Futures for 2025*, Air University Press, Maxwell AFB, AL, 1996, table 6, page 210.

² *Storm Over Iraq, Air Power and the Gulf War*, Richard P. Hallion, Smithsonian Institution Press, Washington & London, 1992, page 169.

Notes

³ *Jane's Space Directory*, 12th Edition, Biddle's Ltd. Great Britain, 1996, page 160.

Chapter 3

A Military Communications Satellite History

In order to better understand the significance of today's shift to commercial platforms, it is first important to be familiar with the thirty-one year history of military satellite communications and the associated equipment that continues to serve as the military's communication foundation. Therefore, the first priority is to detail a concise history of military communications satellites from first launch through the development of the five platforms that have been and are the current foundation of military satellite communications. Having done that, the significance of the shift to commercial satellites should become evident.

In the Beginning

The idea that earth-orbiting satellites could be used for communications is popularly attributed to Arthur C. Clarke. In 1945 he published an article discussing the use of the German V-2 rocket for Ionospheric research in which he also said:

"An artificial satellite at the correct distance from the earth would make one revolution every 24 hours; i.e. it would remain stationary above the same spot and would be within optical range of nearly half the Earth's surface. Three repeater stations, 120 degrees apart in the correct orbit, could give television and microwave coverage to the entire planet."¹

From that conceptual beginning sprung a communications satellite infrastructure that may have even surprised Clarke. The first satellite of which was launched just thirteen years after Clarke's ideas were published.

The United States orbited its first communications satellite, SCORE (Signal Communication by Orbiting Relay Equipment), in 1958. This satellite was nothing more than a tape recorder and a transmitter that allowed the broadcast of a pre-recorded Christmas message from then-President Eisenhower. SCORE remained active for thirteen days before falling silent. Two years later, Courier was launched. Its activity lasted seventeen days and it featured the first active repeater. Messages could be uploaded and recorded as Courier passed overhead and then played back and downloaded as it passed overhead the intended receiver. This arrangement required at least two orbits to send and receive a response, a period of between 90 and 120 minutes. Although impractical for time-sensitive communications, it was a marked advancement over SCORE and paved the way for the first truly useful US military communications satellite system. That practical system was launched six years later when the first seven Defense Satellite Communications System (DSCS), phase one, satellites reached orbit.²

DSCS

DSCS I was a highly successful satellite series that provided secure communications to a variety of customers. In order of precedence, DSCS supported Presidential communications, World Wide Military Command and Control System (WWMCCS), unified commanders, Joint Chiefs of Staff, Defense Information Service, early-warning sites, intelligence sources, diplomatic data and voice, Navy ship to shore, the United Kingdom and NATO. The series included twenty-six individual satellites and in addition

to designed capabilities, was responsible for the transmission of high-resolution photographs between South Vietnam and Washington until the late 1960s.³ The DSCS satellite weighed in at just less than 100 pounds.

First launched on a Titan 3C, DSCS I satellites (and all subsequent military communications satellites) were placed in geostationary orbit - an orbit located above and in line with the equator at an altitude of about 22,238 miles, at a velocity of 6,879 miles per hour. In this orbit, movement is "synchronized" with the earth below. The satellite appears to remain stationary in the sky, while actually completing one orbit every 24 hours. All geostationary satellites are stationed above the equator at the same altitude, spaced around a circle about 165,000 miles in circumference. They are carefully separated by distance or by assigned radio frequencies to prevent interference between their individual communications systems.⁴ In the case of DSCS I, it was determined that a constellation of twenty-six different satellites, spaced in geostationary orbit, was necessary to give worldwide coverage.

The DSCS I follow-on, or DSCS II, was first launched in 1971. It included the same basic capabilities in DSCS I, but added capacity. It also had provisions for satellite repositioning while in orbit. Its launch weight was more than ten times that of DSCS I weighing in at 1,146 pounds. A total of fifteen DSCS II were launched, eleven of which successfully reached useable orbits. The other four were either destroyed in launch accidents or placed in unusable orbits.⁵

DSCS III was first launched in late 1982 and was the first in the series to offer anti-jamming capabilities and improved communications security. Solid-state amplifiers replaced the wave tubes found in DSCS I and II. A total of seven has been launched, all

successfully, and remains on station today providing the bulk of Department of Defense communications. DSCS III weighs approximately 5,765 pounds.

FLTSATCOM

First launched in 1978, FLTSATCOM was a US Navy effort to provide UHF (ultra-high frequency) and SHF (super-high frequency) transponders for high-priority UHF communications between naval aircraft, ships, submarines, and ground stations. In addition, the satellite also provides the Air Force with communications channels used for the AFSATCOM (Air Force Satellite Communications) which facilitated secure communications between the national command authority and nuclear capable assets.⁶ Together the FLTSATCOM and AFSATCOM provided positive command and control of US alert nuclear forces. The US Navy Space and Naval Warfare Systems Command (SPAWAR) was the program manager, responsible for all engineering and acquisition. Payload integration, launch, tracking and data acquisition, was the responsibility of the US Air Force's Space Systems Division.

Although a total of eight FLTSATCOMs were launched, one was destroyed due to a launch booster failure; and, a second was made inoperative when the satellite shroud collapsed during launch operations destroying the primary antennae.⁷ Two other satellites have exceeded their design life and are retired. Of the remaining four FLTSATCOMs, two are in service, and two are in on-station reserve and can be activated as required by ground stations.

LEASAT

The third major US military communications satellite program was LEASAT (Leased Satellite). The program was initiated as a result of Congressional reviews in 1976 and 1977 that advised increased use of leased commercial facilities. It was envisioned as a system to augment the already in-service FLTSATCOM. Owned by Hughes Communications, the satellites were designed to provide global UHF communications to air, sea, and ground forces. The system's primary user is the US Navy who pays Hughes \$84M per year for each operational satellite. At the end of each satellite's designed seven-year life, the Navy has the option of purchasing the satellite for \$15M.⁸

A total of five LEASATS were launched beginning in 1984. All launches were made via the Space Transportation System (Space Shuttle) and placed in low Earth orbit (LEO) after which an attached inertial upper stage (IUS) booster placed the satellites in their permanent geostationary orbits (GEO). LEASAT number 4, although successfully delivered by the space shuttle to LEO, failed to attain GEO due to an inertial upper stage (IUS) failure.

Like FLTSATCOM, the Air Force utilizes a portion of the narrow-band channels for AFSATCOM requirements. And, also like FLTSATCOM, the US Navy serves as program manager while the Air Force is responsible for launch and post-launch control functions as well as the day-to-day flight profile maintenance. The combined FLTSATCOM, LEASAT constellation accounts for approximately ninety percent of Navy communications.

Ultra-High Frequency Follow-On

The Ultra-High Frequency Follow-On (UFO) program is a replacement for the FLTSATCOM/LEASAT program replicating all the aforementioned capabilities. In addition, the system will provide double the communications capacity, improved protection against electronic threats and will provide an interim Global Broadcast Service (GBS) via onboard GBS transmitters on satellites eight through ten.⁹ The full operational network will consist of eight satellites initially controlled by the Air Force with a control responsibility transfer to the Navy's Point Mugu Navy Satellite Operations Control Center in 1999 after the last launch. As part of its survivability features, UFO has also been designed to operate for up to thirty days without ground contact.¹⁰

The first UFO launch was in 1993 but due to booster failure, did not achieve usable orbit. Launches two through seven were successful in placing UFOs in geostationary orbits. With a configuration similar to its predecessors, UFO continues the pattern established with FLTSATCOM and LEASAT and completely supports AFSATCOM nuclear control channel requirements. Later UFO platforms also include extreme high frequency (EHF) transponders to provide compatibility with future MILSTAR configurations. UFO's dramatically increased capacity allows the Navy to provide previously unavailable shipboard services including direct broadcast of entertainment channels to shipboard receivers.

MILSTAR

MILSTAR is the next generation military communications satellite system. In addition to possessing all the capabilities of FLTSATCOM, LEASAT, and UFO, its hallmark features are its anti-jamming and survivability systems. It is electro-magnetic

pulse hardened, nuclear shielded, and has the ability to alter orbit parameters to move itself out of harm's way. To resist jamming, it employs an EHF frequency-hopping scheme whereby broadcast messages are sent in microsecond bursts, each one on a different and apparently random frequency. Only a receiver with the appropriate frequency-hopping algorithm is able to reconstruct the original message. MILSTAR also features on-board processing. This allows jammed or altered signals to be electronically "cleaned" onboard and then retransmitted and amplified without the incoming message corruption. Rounding out the enhanced MILSTAR capabilities is the ability to crosslink. All predecessor systems relied on ground receivers to pass signals between orbiting spacecraft. For instance, if a Pacific ship wished to send a SATCOM message to a user in the Atlantic, the message would first go to an orbiting satellite; then, down to a ground station then up to the next satellite and so forth until the message eventually would get to a satellite overhead the Atlantic receiver. MILSTAR changes all that because of crosslinking. In addition to antennae pointed towards terrestrial users, it has antennae pointed towards the adjacent satellites, both left and right, in the orbital plane. This allows MILSTAR to pass message traffic directly from satellite to satellite until it gets to the platform directly overhead the intended receiver. This system eliminates the requirements for multiple ground-based receiving stations, a benefit that results in faster transmissions, increased security, and less reliance on other countries to support US ground-station needs. There is a down side, however, and that is fiscal. The first MILSTAR satellites cost about \$1 billion each to build and launch.

Although two MILSTAR I satellites have been successfully launched, subsequent launches will place MILSTAR II spacecraft in orbit - a lower-priced, slimmed down

model that does not have the nuclear-hardening characteristics of the block one platforms. Final constellation completion is not scheduled until after 2006.

These then are the major US military communications satellites past and present. All of these systems have been designed, built, launched, controlled, and maintained by the United States. All system users are granted access exclusively by the United States. This degree of control enhances our national ability to ensure uninterrupted communications integrity, security, and access. It does not, however, guarantee it.

Notes

¹ Clarke, Arthur C., *A Scientific Autobiography, Ascent to Orbit*, John Wiley and Sons, 1984, pages 53-58.

² *Jane's Space Directory*, 12th Edition, Biddle's Ltd., Great Britain, 1996, page 161.

³ *Jane's C4I Systems*, Biddle's Ltd., Great Britain, 1996-1997, page 133.

⁴ NASA Quicklink, <http://spacelink.nasa.gov/NASA.projects/satellites/fltsatcom.net-work>

⁵ Mike's Spacecraft Library, <http://www.newspace.com/ref/msl/programs/dscs.html>

⁶ Mike's Spacecraft Library, <http://www.newspace.com/ref/msl/Quicklooks/fltsatcomQL.html>

⁷ Larry's Utility World, <http://www.grove.net/-larry/milsats.html>

⁸ Mike's Spacecraft Library, <http://leonardo.jpl.nasa.gov/msl/Quicklooks/leasantql.html>

⁹ DOD Space Executive Overview, <http://www.acq.osd.mil/space/programs/execsum/uhf.html>

¹⁰ *Jane's Space Directory*, 12th Edition, 1996-1997, Biddle's Limited, Great Britain, page 163.

Chapter 4

Targeting Options

Both the US and our potential adversaries understand traditional system vulnerabilities (“traditional” as differentiated from “new” system vulnerabilities) and have explored ways to exploit those vulnerabilities. To better understand how an adversary might attempt to deny communications, it is helpful to divide satellite communications systems into the following four segments: satellite link, ground link, control link, and user link. Denying any one of these segments denies the entire system. Although any segment can be targeted, the relative ease, military utility, and political acceptability associated with attacking a given segment differ greatly.

Satellite Link (target the flags, banners, bells, and drums)

To some the most obvious target for denying satellite communications is the satellite itself. This attack mode usually involves satellite destruction or incapacitation. Such an approach is highly effective in denying communications to all users of the targeted satellite, effectively rendering that portion of the adversary’s system inoperative. Although effective, this approach is highly expensive, technologically difficult, and irreversible. Despite these considerations, both the United States and the former Soviet Union have pursued anti-satellite (ASAT) programs as a means to deny not only communications, but all other satellite-based capabilities as well. Although the US direct-

ascent ASAT program was terminated in 1988¹, the US Army is currently developing the Mid-Infrared Advanced Chemical Laser (MIRACL) and in the fall of 1997 secured Secretary of Defense permission to test fire the system at an orbiting military satellite.² Although the weapons employment aspects of this satellite control segment are intriguing, the vital element to remember is that destroying or incapacitating the satellite link denies communications to all users of the targeted satellite. Although this would be precisely the intent when targeting a satellite that serves only one function, one organization, or one state, it would not be so acceptable were the satellite shared.

Ground Link (target the tactical unit commanders)

The ground link refers to the equipment and resources that make the connection between communications users and the communications satellite. Typically this segment takes the form of antennae, signals processors, terrestrial-based communications networks, and the gateways that form the interface between terrestrial networks and the satellite networks. Typically too, there are a number of ground segments, one or more for each geographic region the satellite operator wishes to provide communications coverage. Targeting the ground link requires none of the expensive, high technology approaches required when attacking the satellite link. Ground links are typically stationary sites built around an antennae or antennae array. Destroying or incapacitating the site can be accomplished by airborne weapons systems or relatively small groups of foot soldiers. While targeting the ground link itself is usually not a difficult task, gaining access to the terrain surrounding the site may be. By their very nature, ground links are typically sited well within national boundaries of states friendly with the satellite operator.

Control Link (target the communications officer)

Command and Control links refers to the resources and equipment that transmit maintenance, upkeep, and navigational instructions to the orbiting communications satellite. Virtually all military communications satellites are handled by a primary command and control center but they can typically also be controlled from at least one alternate site. Targeting the control link is similar to targeting the ground link. Actual targeting is relatively straight forward; but, gaining unchallenged access to the vicinity of the physical command and control site is much more difficult.

User Link (deafen and blind all the soldiers)

The user link refers to the resources and equipment operated by the intended recipient of satellite communications. It may be a portable or hand-held receiver; or, some other form of mobile user terminal. Targeting the user link is a viable option when the number of targeted users is relatively small. It is not so viable when there are great numbers (as was true with the Chinese army).

Notes

¹ *Military Space*, Brassey's Air Power: Aircraft, Weapons Systems, and Technology Series, Volume 10, 1990, U.K. page 159.

² <http://pathfinder.com/@@R1lxcgUALRoLe8OR/news/latest/RB/1997Sep02/602.html>

Chapter 5

Defending the Resource

Defending the communications satellite system requires an appreciation for the same system segments described in chapter four: satellite link, ground link, control link, and user link. Physically protecting or hardening each component link is the typical approach that communication satellite owners have pursued. The US military has explored options for maneuvering satellites from potential anti-satellite adversaries, physically protecting ground links through barriers and monitoring, hardening, protecting and making control links redundant, and providing perimeter security for the user links. It is a resource protection challenge not unlike that facing any multi-node military system. What makes the future of communications satellite system targeting and protection very different started with the events of 1963.

Parallel Development Paths

It is helpful to understand why the United States pursued parallel communications satellite development with the military charting a course very separate from the civil sector. Well after establishment of the DSCS program, President Kennedy created the National Communications System (NCS) in 1963 in an attempt to assure necessary communications for the Federal Government under all conditions. As agent for the NCS, Secretary of Defense McNamara made inquiries about potential civil-military

communications satellite cooperation. Prior to this, the Defense department did not consider the viability of a commercial system that served defense needs because of beliefs that military requirements were unique and that civil industry would neither be able nor interested in such an effort. On the commercial side was the argument that the international communications satellite effort headed by the Commercial Satellite Corporation (COMSAT) was incompatible with Defense Department participation. Because the US was interested in creating an international communication system, it was thought that US Defense Department participation would be unwise, adversely affecting the attitudes and actions of potentially interested foreign governments.¹ Defense Department reluctance and political caution then worked together to keep military and commercial on the separate paths established prior to NCS formation. Although the DOD leased commercial communications satellite capacity to allow for surge and augmentation purposes, these parallel paths, each well serving its customers, continued essentially unchanged for the next twenty-five years and might have continued indefinitely were it not for the fiscal realities associated with US armed forces downsizing.

Full Circle

In both 1989 and 1990, the Congress issued reports critical of Defense Department management of military satellite communications with an emphasis on the associated high costs. The reports directed DOD to prepare a comprehensive, affordable architecture that defined all satellite communications requirements and potential solutions to satisfy the requirements. The DOD responded in November 1991 with an architecture study which included the alternative of using commercial communications satellites. This approach was also consistent with the White House issued National Space Policy

Directive 3 which required US government agencies to use commercially available space products and services to the fullest extent feasible as a means towards reaping economic benefits.²

One of the key elements in the DOD report was the defining of “core” versus “general” communications requirements. “Core requirements” referred to critical communications necessary for commanding and controlling combatant forces in stressed environments. General requirements were less critical or less time-sensitive communications in unstressed environments that involve, for example, transmissions of logistics, administrative, and intelligence data and do not call for highly jam-resistant capabilities, making commercial communications satellites highly suitable for satisfying such requirements.³ In the years since issuing this report, however, the DOD has found it much easier defining core and general requirements than it has estimating how much of its communications fall into which category. Because individual military units pay directly only for general communications, there appears to be a tendency for units to categorize some communications as core that would easily fall into the general category were it not for the associated fiscal benefit when the unit uses core versus general resources. Further clouding the picture is the way the DOD procures commercial communications satellite services. There is currently no central contracting agency buying “in bulk” with the associated benefits. Individual units often contract directly with communications providers making the capture of usage patterns and volumes virtually impossible.⁴

In response to the fiscal Year 1992 House Appropriations Committee Report (which directed the DOD to study how commercial satellite systems could meet future

department needs), the DOD established the Commercial Satellite Communications Initiative (CSCI). The CSCI sought to explore, validate, and institutionalize the role of commercial solutions to DOD's communications requirements. Industry was a partner in the study and contributed significantly to the resulting conclusions. Not surprisingly, the results, as reported in the June 1994 Report to Congress, were along the same mission lines described in the 1991 architecture study: core and general requirements. The DOD and industry both recommended that the government procure and be responsible for protected (core) communications and that unprotected requirements (general) could be satisfied by commercial industry.⁵

Security Concerns

Although the CSCI acknowledged the fiscal benefits and technological feasibility of pursuing commercial solutions to military communications needs, it also made important references to specific threats associated with military reliance on commercial communications systems. The Naval Security Group (NSG) handled the CSCI information warfare aspects. It concluded that the most significant vulnerability to DOD in using commercial satellite communications was susceptibility to exploitation. In its recommendations is specifically mentioned avoidance of cellular telephone SATCOM systems.⁶ The next chapter description of Iridium, the newest world-wide cellular technology, will help the reader to better understand the NSG concern.

Notes

¹ Galloway, Jonathan F., *The Politics and Technology of Satellite Communications*, Lexington, Massachusetts, Lexington Books, 1972, page 107

² *Military Satellite Communications: DOD Needs to Review Requirements and Strengthen Leasing Practices*, United States General Accounting Office Report 94-48 to

Notes

the Chairman, Subcommittee of Defense, Committee on Appropriations, House of representatives, February 1994, page 1.

³ Ibid.

⁴ Ibid., page 3

⁵ *Report to Congress on the Commercial Satellite Communications Initiative*, Department of Defense, June 1994, page 8.

⁶ Ibid., page 18

Chapter Six

The Iridium Case

Iridium is a communications satellite service designed by Motorola and built, fielded, and operated by a multi-national consortium. When fully operational in 1998, Iridium will provide its subscribers with global cellular telephone service. The system will operate like this: An Iridium subscriber will place a call by activating a handset looking much like today's cellular phones. If the subscriber chooses, the call will be processed as a standard cellular call using existing cellular networks and tie-ins to standard switched telephone networks. If the subscriber is not in range of a traditional cellular network; or, simply elects to choose a satellite-direct call path, the closest satellite in Iridium's 66-satellite low-earth-orbit (LEO) constellation receives the signal. If the call's intended receiver is another Iridium subscriber mobile in the same coverage area, the signal will be relayed directly to that subscriber's handset completing the handset-to-satellite-to-handset circuit. If the intended receiver is not another mobile Iridium subscriber, the call will be routed from the satellite to the existing terrestrial switched telephone network serving the receiver. During the course of the telephone call, communications segments handled by orbiting Iridium satellites will be seamlessly handed-off from satellite to satellite as each subsequent satellite comes into the caller's view. The constellation also has the capability to cross-link calls from satellite to satellite

allowing completion of calls from any two points on the globe. In the case of a call between two mobile Iridium customers, the connecting would travel exclusively on orbiting satellites. All other calls would rely on at least one segment being routed through existing terrestrial telephone networks.

Terrestrial switched telephone networks will connect with Iridium satellites through Iridium gateways. Designed to be transparent to the user, Iridium gateways will handle the transition from terrestrial network to satellite network in like manner as current cellular telephone system gateways handle the transition from terrestrial networks to tower-mounted cellular antennae systems. Iridium gateways will be owned and operated by Iridium, Incorporated investors. The investors include companies from Saudi Arabia, Canada, China, India, Venezuela, Russian Federation, Republic of Korea, Japan, Germany, Taiwan, Indonesia, Italy, and Thailand. With the exception of Iridium mobile handset-to-handset calls in the same geographic area, all Iridium calls will be handled by at least one of the Iridium gateways.¹

Although not marketed as an Iridium “feature,” the system employs sophisticated subscriber location technology that makes it possible for the Iridium system to geographically locate any given customer worldwide. This capability allows the system to know through which satellites to route in-comings calls. Each cellular handset has a unique identification code to facilitate the locating feature. An Iridium promotion explains it this way: “Even if an Iridium subscriber’s location is unknown, the system will provide global transmission by tracking the location of the telephone handset.”² This Iridium system description should suggest to the reader three fundamental challenges for

the military user: foreign control, targeting ambiguity, geo-location. Each presents specific problems that warrant careful consideration.

Foreign Control

With system ownership shared in part by Saudi Arabia, Canada, China, India, Venezuela, Russian Federation, Republic of Korea, Japan, Germany, Taiwan, Indonesia, Italy, and Thailand, it is not difficult to imagine alternative futures in which the United States would have a conflicting national agenda with at least one of the consortium players. Were this to happen, what technological leverage might consortium members have against those interests? Denial or impeding of US communications is certainly the first possibility that comes to mind. Would a potential consortium adversary be able to degrade the entire system by shutting down one or more of the state-owned strategic gateways, saturating the overhead system with spurious or nuisance information, or subjecting associated terrestrial networks to monitoring or degradation? While denial or degradation of US communications may be the most direct approach to applying technological leverage, there are other less direct but nevertheless effective courses of action available to a potential adversary. Imagine the potential impact of a consortium member's isolating a city, state, or region through denying cellular communications. Although less likely to be effective in the highly developed countries, imagine the impact in less-developed areas where the new global cellular connectivity provided by systems like Iridium is the only communications source available. Could it happen? It has already happened. Consider the events of late summer 1997 in the Chechen capital, Groznyy,

Communications Isolation

According to a spokesman for the Chechen leadership, an information blockade of the Chechen Republic began in August when the Russian Federation switched off all cellular telephone communications effectively making contact with the outside world non-existent.³ Although the Russian Federation asserted that the disconnection had no political grounds, it did acknowledge that for fiscal reasons (the Chechens were behind in their cellular payments) the system had been shut down.⁴ Whether politically motivated or not, the service disruption was real and Chechnya was effectively communications isolated.

Remember, the local Iridium investor owns all Iridium gateways; and, although cellular handset-to-handset calls can go direct, the majority of calls will make some portion of the linkup through the Iridium gateways. Could the Chechen scenario repeat somewhere else? Apparently the US government believes so and it has invested a reported \$56 million to build a DOD-only Iridium gateway on US soil so that government-military communications can continue unaffected by regional gateway shutdown. This, however, places all the eggs in one basket by making the US government gateway a single-point failure node. And, unless other regional governments, coalition militaries, and interests are also given access to the US government gateway, there may not be anyone to talk to.

Targeting Ambiguity

Should the United States find it useful to denying a potential enemy its communications doing so in an “Iridium” world will be a very different challenge. What can be targeted given the shared resource? The traditional space control segments which

include the satellite link, ground link, control link, and user link become less definitive, less available. Target the satellite link and you target your own satellite. Target the ground link and you may disrupt friendly communications transiting the same networks. Target the control link and you target your own system as well. The only apparently viable option becomes targeting the user segment and that has its own complexities of scale. This is not to suggest that targeting the communications system is no longer an option. Targeting must, however, be redirected and rethought outside of traditional space-control boundaries. In most scenarios successful targeting will depend upon having access to and cooperation with the satellite infrastructure architects and operators.

Geo-location

Perhaps the most intriguing military potential of the Iridium system is suggested in Iridium's own promotion where it offers that, "Even if an Iridium subscriber's location is unknown, the system will provide global transmission by tracking the location of the telephone handset."⁵ While this capability is understandably important for directing calls to an intended receiver, it suggests a very real military capability: the ability to locate a target receiver anywhere in the world virtually undetected. The ability of the US military to access, process, digest, and act upon this information is essential not just to developing target solution sets but to understanding the ways that an adversary might attempt to use the same information. The US military decision to build and operate its own Iridium gateway greatly lessens but does not eliminate the vulnerability to global precision attack based on cellular handset geo-locatability. Not all military users, however, will access the military gateway.

Private Proliferation

It will, no doubt, be the military's intention to have all its Iridium users go through the designated military gateway. History suggests that this will just not happen. Consider the infamous and nationally publicized pay-telephone calls to headquarters made during the US Grenada invasion when tactical communications were not yet available. Consider, too, the numbers of cell phones that US citizens, including military private citizen, buy and operate today to satisfy their private communications needs. Is it reasonable to expect that these consumer-model cellular handsets will not find their way to future conflict areas, especially given the new, worldwide connectivity capabilities promised by Iridium in 1998? Unless commanders make specific and vigilant efforts preclude the introduction of personal communications assets, like Iridium handsets, into deployed theaters of operation, infiltration and proliferation will occur. And, when it does, potential adversaries will have the capability to exploit geo-location features to determine U.S. force composition and location.

System Dependence

If the fact that the US government is building its own Iridium gateway does not alone suggest a deep commitment to and dependence on the Iridium system, consider this extract the United States Army's Battlefield Information Transmission System Far Term Strategy (version 2.0), 1 September 1997. "Satellite Personal Communications Systems will allow the Army to leverage and exploit emerging commercial satellite systems to provide a cost effective, military enhanced, highly mobile, handheld, secure, flexible, intra-theater, and worldwide capability for those warfighters who may be otherwise isolated from established military or commercial networks.⁶ The strategy specifically

references Iridium as a candidate emerging system. The strategy asserts that communications will be secure but does not address the issue of geo-location.

Not Just Iridium

Were Iridium the only global-wide, international-consortium-owned communications satellite system planned for the near future, meeting the already-mentioned security challenges would be somewhat easier. It is, however, not the only planned system. Logarithmically increasing the military challenge will be systems such as Teledesic, which is currently planned, funded, and scheduled for service within the next five years. Teledesic will rely on more than 233 low-earth-orbit satellites and will provide worldwide users with high-speed data and Internet access. The military security implications will be correspondingly challenging.

Notes

¹ <http://www.iridium.com/proflle/invdes.html#thai>

² <http://www.iridium.com/systm/sysgat.html>

³ Moscow Denies Chechen Republic's Communications Cut, Moscow Radio, 1505 GMT, 2 Oct 97, FBIS translation from the Russian, http://www.au.af.mil/FBIS/Articles/1997/10/06/Central_Eurasia/3295955883.html

⁴ Russian Official View Chechen Cellular Communications, Moscow TASS News Agency, 1558 GMT, 3 Oct 97, in English, FBIS translated text, http://www.au.af.mil/FBIS/Articles/1997/10/07/Central_Eurasia/1754456809.html

⁵ <http://www.iridium.com/systm/sysgat.html>

⁶ United States Army's Battlefield Information Transmission System Far Term Strategy (version 2.0), 1 September 1997, <http://fotlan5.fotlan.army.mil/BITS/bits.html>

Chapter Seven

Recommendations

Given the general increase in military reliance on commercial communications satellites and the specific reliance on systems like Motorola's Iridium, military planners should consider the following as a means towards improving an ability to successfully adapt to the new "rules."

1. Exercises and Simulations: Amend exercise and simulation scenarios to include adversarial use of the same satellite communications constellations used by U.S. forces. Include situations that require commanders and planners to address the associated targeting and defense issues.
2. OPLAN amendments: After sufficient simulation and exercise play identifies the necessary new approaches to both targeting and defending internationally shared communications satellite constellations, develop and then codify the strategies necessary to deal with this new situation.
3. Private Cell-Phone Proliferation: Educate commanders and planners on the potential and associate risk of hostile geo-location based upon even non-military use of privately owned and operated satellite-based cell phone usage (like Iridium).

Chapter Eight

Conclusion

The Congressionally mandated shift of general military communications from organic to commercial satellites is no longer just a plan. It is a reality that provides the military with both tactical and strategic challenges that will shape the character of future information warfare. Commanders and war planners alike are learning to embrace, understand, and incorporate these new technologies. The concern is whether commanders and war planners will have a corresponding understanding of and appreciation for the new ways of thinking that must accompany the new technology. Specifically, the military migration to consortium financed and owned commercial communications satellite systems is precedent setting. It marks the first time that the U.S. military will have major reliance on a single system that also may be serving potential adversaries. A renaissance in military thought must accompany this renaissance in military affairs.

Although the issue is different and the challenges new, there remains a constant that characterizes military technology changes. That constant was well described by Air Marshall Giulio Douhet: “Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.”¹

Increased military reliance on commercial communications satellites is a situation much in need of thoughtful anticipation of the associated changes in the character of war.

Notes

¹ Douhet, Giulio, Italian Air Marshall, 1928, *Contrails*, Vol 17, 1971-1972, USAFA, Colorado, page 227.

Bibliography

Alternate Futures for 2025, Air University Press, Maxwell AFB, AL, 1996.

Clarke, Arthur C., *A Scientific Autobiography, Ascent to Orbit*, John Wiley and Sons, 1984

Department of Defense, *Report on the Bottom-Up Review*, October 1993

DOD Space Executive Overview, <http://www.acq.osd.mil/space/programs/execsum/uhf.html>

Douhet, Giulio, Italian Air Marshall, 1928, *Contrails*, Vol. 17, 1971-1972, USAFA, Colorado.

Galloway, Jonathan F., *The Politics and Technology of Satellite Communications*, Lexington, Massachusetts, Lexington Books, 1972, page 107

Hallion, Richard P. *Storm Over Iraq*, Air Power and the Gulf War, , Smithsonian Institution Press, Washington & London, 1992.

<http://www.iridium.com>

Jane's C4I Systems, Biddle's Ltd., Great Britain, 1996-1997

Jane's Space Directory, 12th Edition, Biddle's Ltd. Great Britain, 1996, page 160.

Kaminski, Paul, *Investing in Tomorrow's Technology Today*, Defense Issues, Volume 10, Number 46, March 28, 1995

Larry's Utility World, <http://www.grove.net/~larry/milsats.html>

Memorandum for Under Secretary of the Army, The Army Enterprise Strategy, The Implementation Plan, <http://www.hqda.army.mil/enterprise/implplan/vcsaltr.htm>, July 1993.

Mike's Spacecraft Library, <http://www.newspace.com/ref/msl>

Military Satellite Communications: DOD Needs to Review Requirements and Strengthen Leasing Practices, United States General Accounting Office Report 94-48 to the Chairman, Subcommittee of Defense, Committee on Appropriations, House of representatives, February 1994.

Military Space, Brassey's Air Power: Aircraft, Weapons Systems, and Technology Series, Volume 10, 1990, U.K.

Moscow Denies Chechen Republic's Communications Cut, Moscow Radio, 1505 GMT, 2 Oct 97, FBIS translation from the Russian, http://www.au.af.mil/FBIS/Articles/1997/10/06/Central_Eurasia/3295955883.html

NASA Quicklink, <http://spacelink.nasa.gov/NASA.projects/satellites>

Report to Congress on the Commercial Satellite Communications Initiative, Department of Defense, June 1994.

Report to the Chairman, Subcommittee on Defense, Committee on Appropriations, House of Representatives, Military Satellite Communications, February 24, 1994.

Report to the Secretary of Defense, Defense Satellite Communications, Alternatives to DOD's Satellite Replacement Plan Would Be Less Costly, July 1997.

Russian Officials View Chechen Cellular Communications, Moscow TASS News Agency, 1558 GMT, 3 Oct 97, in English, FBIS translated text,
http://www.au.af.mil/FBIS/Articles/1997/10/07/Central_Eurasia/1754456809.html
Sun Tzu, *The Art of War*, Samuel B. Griffith, Oxford University Press, Oxford, 1963

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air War College
Maxwell AFB, AL 36112